Multimedia Section

TRAINING PROGRAM MANUAL

DIGITAL EXAMINATIONS

Digital and Multimedia Evidence Division

1. Scope

Education and training form the cornerstone for achieving excellence in the delivery of highly reliable and repeatable digital forensic services. The management of the Houston Forensic Science Center (HFSC) is committed to excellence by initiating, supporting, and adhering to this training program intended to develop staff technical skills through a set of relevant and comprehensive training activities.

This training manual and the overall training program is applicable to management and technical staff of the Multimedia Section. The training program includes basic HFSC orientation training, training and development of digital forensic skills, competency and proficiency testing, continuing education, and advanced technical skills training and certification. This program defines requirements for the career development of analysts from the basic levels of technical services to the professional development of expert level competencies. The newly hired analyst (whether experienced or not experienced) will be referred to as “trainee” throughout this training manual. They have been employed by HFSC after meeting the requirements of education, experience, and skills listed in the job description and who have passed the required background check and drug screen.

This training manual is organized into modules in specific areas of digital analysis and administrative functions. Modules pertaining to types of examinations do not need to be completed in a specific order. Competency tests will be administered prior to supervised casework and mock trials. Mock trials should be the last module completed prior to authorization for casework.

1.1 Training Program

As the trainee progresses toward independent casework, the training program will remain specific to the trainee’s forensic sub-discipline. In situations involving newly-hired analysts who have already been performing casework for other laboratories or organizations, the newly-hired analyst’s competency will be assessed, and the training program modified accordingly. At a minimum, new analysts will complete a competency test prior to performing casework. In any training program, additional training tasks and supervised casework may be included at the discretion of the trainee or supervisor/lead.

This training manual along with other materials generated during the training program shall be retained in a binder and/or electronically. All training checklists, authorization memos, and module completion dates will be documented.

1.2 Trainers

Trainers are qualified analysts who are assigned by section management to provide direct day-to-day training and guidance to digital forensic trainees. They have been authorized to perform the tasks described in the module(s). Refer to the trainer’s Q-file to see the specific areas the trainer is authorized in. The trainer’s primary goal is to guide trainees in performing their technical and administrative responsibilities. Trainers strive to facilitate professional and technical development of the trainee. They work closely with the section’s supervisor/lead and manager to ensure that the training program is effective and relevant, offering suggestions for improvement as needed.

The development of a trainee's knowledge, skills, and abilities under the guidance of their mentor are documented in this training manual which serves as an official record of the progress for each trainee undergoing development. The trainer is responsible for verifying the trainee's skills and abilities to perform specific administrative and technical tasks as documented in this record. The trainee may have more than one trainer through the training program.

1.3 Performance Verification of Hardware/Software

In certain modules the trainee will be performing verifications of hardware and software that is assigned to him/her. In order to verify the hardware/software, the trainee will use the section's data sets and the procedures will mimic casework.

1.4 Competency

All trainees must successfully pass a comprehensive competency test which will be referred to as practical exams in this manual. Competency testing can be conducted either at the end of the training program or in a modular format throughout the course of training. At any point when a trainee learns a new technique and/or process, to perform their duties, their competency in that area will be tested:

- These levels are driven by the requirements established in the forensic community for the specific tasks to be accomplished.
- This curriculum is designed to provide the skills and information necessary for the trainee to attain competency in the areas of digital forensic analysis.

1.5 Practical Competency Exam

The practical competency exam consists of conducting analysis on known evidence with a known outcome predetermined by the trainer/supervisor. The trainee is required to: correctly identify the relevant issue(s), select appropriate software and/or hardware tools to conduct the analysis, and produce an appropriately processed output result. If the trainee does not meet all three of the criteria, then a second competency exam will be administered. The trainee will produce case notes and any other required documentation for the exam. A report will be issued by the trainee to the findings of the examination. All work must be conducted in compliance with current section and HFSC Quality Manual policies and procedures. If deemed necessary, an oral examination will be provided to test the trainees' ability to define technical processes and terms logically and professionally. A minimum score of 80% is required.   The questions included in the oral examination will be documented by the trainer as well as whether or not the trainee's responses were acceptable.

1.6 Written Competency Test

Each practical competency exam will contain a written test. The written test will contain questions pertaining to the practical case and the trainee must answer the questions accordingly. If the trainee does not pass the written test, a remediation training plan will be created to address the areas the trainee did not pass. A minimum score of 80% is required to pass the exam.

1.7 Remedial Training

If a trainee fails to pass the written, oral, or practical competency exam then they will repeat the training and have one opportunity to retake the exam. If the trainee is still not successful, the supervisor/lead, in conjunction with the manager, will determine the best course of action. The trainee may be required to take additional training courses prior to repeating competency exams.

If a trainee fails to pass a mock trial, the trainee may redo the mock trial up to two times. If the trainee is still not successful, the supervisor/lead, in conjunction with the manager, will determine the best course of action.

1.8 Certifications

Certifications can be comprehensive or topic specific and can be an added tool in verifying analysts' technical skills and abilities. Certifying bodies generally require training and a minimum amount of experience in the discipline in order to sit for an exam. IACIS, SANS, and Cellebrite (for example) certifications for digital analysts in all sub-disciplines in which they conduct casework is encouraged. Maintaining certification may require retesting and meeting specific continuing education requirements. Certain certifications are required to begin casework. Certifications other than the ones listed below can be accepted with approval from the section manager.

For casework authorization in computer analysis the analyst must possess or have received one of the following external certifications and/or degrees:

- EnCase Certified Examiner (EnCE)
- IACIS Certified Computer Forensic Examiner (CFCE)
- GIAC Certified Forensic Examiner (GFCE)
- Master's Degree in related discipline (to be determined by manager)

For casework authorization in mobile device/cell phone analysis the analyst must possess or have received one of the following external certifications and/or degrees:

- Cellebrite Certified Operator (CCO) and Cellebrite Certified Physical Analyst (CCPA) Certifications

- Cellebrite Certified Mobile Examiner (CCME) Certification
- GIAC Advanced Smartphone Forensics (GASF) Certification
- IACIS Certified Mobile Device Examiner
- Master's Degree in related discipline (to be determined by manager)

1.9 Continuing Education

Forensic continuing education provides an analyst with the skills and knowledge of evolving technology in digital and multimedia forensics. Training in specific sub-disciplines and specialized areas may be dictated by the forensic discipline, accreditation status, and/or the requirements of the Houston Forensic Science Center.

Continuing education should be obtained annually from training conferences, trade shows, professional organizational memberships, professional publications, current literature, or specialized courses. Training should address updates and the use of new technologies as it relates to:

- Hardware and equipment
- Software
- Techniques, procedures, and methods

1.10 Proficiency

Once authorized to conduct casework, analysts must successfully pass an annual discipline-specific proficiency test. Proficiency testing is the continual evaluation of all analysts in the performance of tasks relating to their discipline. If compliance with proficiency testing is not achieved, independent casework must cease until proficiency is demonstrated. Refer to the HFSC Quality Manual for information regarding proficiency tests.

1.11 Casework Authorization

Trainees who fulfill all the requirements in the training program and pass the practical competency exams will be issued an authorization memo. The authorization memo will delineate the areas in which the trainee is qualified and authorized to perform analysis. It will also include the software the trainee is authorized to use in that area of analysis.

1.12 Mock trial

Testimony is an important aspect of forensic science and is something that an analyst will be required to give. A mock trial shall be used to determine the trainee's ability to provide effective expert witness testimony. The mock trial will be completed prior to being authorized to perform independent casework.

2. Modules

Module 1 – Administrative and Evidence Handling

Required Reading:
HFSC Quality Manual
HFSC Evidence Handbook
Administrative/Quality SOP
TFSC Evidence Handling Readings
HFSC Policies and Procedures
HFSC Health and Safety Manual
HFSC Security Manual
Multimedia Section SOPs
Digital Evidence and Computer Crime (2nd Edition) – history and basic theory

Objectives:

- Trainee will learn how to use LIMS when creating items of evidence.
- Trainee will learn how to transfer custody of items of evidence using LIMS.
- Trainee will learn Portal and how requests are made and how evidence is brought to the section.
- Trainee will understand the requirements for uniquely identifying, documenting, and controlling digital evidence in addition to requirements for sealing and storing physical evidence.
- Trainee will learn to photograph evidence items for the case record.
- Trainee will read all applicable OSAC standards in the Digital Evidence discipline.

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Required Readings			
Evidence Handling			

Module 2 – Quality Boot Camp

Required Reading:
HFSC Quality Manual
TFSC Root Cause Analysis Readings

Objectives:

- The trainee will attend a quality training course that will be conducted by a member of the Quality Division.
- The trainee will learn about the Quality Management System and ISO/IEC 17025 requirements.
- The following items will be discussed in this training:
  - Accreditation/Scope of Accreditation
  - Document Control
  - Audits
  - Nonconforming Work
  - Root Cause Analysis
  - Personnel
  - Equipment
  - Validations
  - Technical Records
  - Technical/Administrative Reviews
  - Testimony Monitoring
- The trainee will gain a better understanding of documentation in case records.
- The trainee will gain more understanding of how the Quality Management System is managed including the use of Qualtrax to achieve and maintain document control.

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Required Reading			
Quality Boot Camp			

Module 3 - Hard Drive Removal/Write Protection

Required Reading:

Hard Drive Removal Technical Procedure
Technical Procedure for Write Protection of Media
Related Validations/Performance Verifications

Objectives:

- Trainee will remove hard drives from laptops or desktops for data collection and preservation.
- Trainee will use write protection devices to preserve data from physical devices.
- Trainee will use verification (hash) tools from within forensic products to verify physical or logical data (i.e., network) recovered or collected.

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Required Reading			
Performance Verification of Hardware/Software			
Hard Drive Removal/ Write Protection			

Module 4 – Imaging/Wiping

Required Reading:
Physical and Logical Imaging Technical Procedure
Technical Procedure for Wiping Media
Related Validations/Performance Verifications

Objectives:

- Trainee will use imaging hardware and forensic software to collect and preserve data from physical devices.
- Trainee will use hardware and software to forensically wipe devices of data.

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Required Reading			
Performance Verification of Hardware/Software			
Imaging/ Wiping			

Module 5 – Computer/Laptop Technical Skills

Required Reading:
Hard Drive Removal Technical Procedure
Technical Procedure for Write Protection of Media
Physical and Logical Imaging Technical Procedure
Technical Procedure for Wiping Media

On-Site Forensic Previews SOP
Related Validations/Performance Verifications

Objectives:

- Trainee will recover and collect electronically stored physical and logical level data from devices and/or networked computers which may include the machine BIOS, Windows Registry, active files and folders, deleted files and folders, Pagefile data, unallocated data recovery, data carving, social network artifacts and transactions, email and email attachments, link file analysis, file metadata extraction, temporary file activity, and browser history and activity.
- Trainee will understand common Windows file structure, Microsoft Office applications, and concepts for data storage on internal and external devices, the characteristics of electronic stored information (i.e., logical and physical data on a hard drive) vs. Redundant Array of Independent Disks (RAID) storage (i.e., server logical data), and the methods to identify and analyze computer activity (e.g., forensic artifacts, metadata, timelines, etc.).
- Trainee will understand the technical processes and procedures to preserve and collect data from physical devices such as hard drives, laptops, and desktop computers using approved hardware and software.
- Trainee will understand the most common data structures and server architecture to facilitate basic collection of electronically stored information.
- Trainee will use forensic analysis tools to filter and sort data based upon file types, dates, special characters (e.g., credit card number), text searches, and password recovery and/or cracking.
- Trainee will use other tools to collect and recover relevant data requested by the stakeholder while maintaining the integrity of the data.
- Trainee will learn how to preview devices at off-site locations (i.e. search warrants) for evidentiary value.

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Required Reading			
Performance Verification of Hardware/Software			
Computer/ Laptop Technical Skills			
On-Site Forensic Previews			

Module 6 – Mobile Device Extractions

Required Reading:
Mobile Device Data Extraction SOP
Physical and Logical Imaging Technical Procedure SOP
On-Site Forensic Previews SOP
Related Validations/Performance Verifications

Objectives:

- Trainee will recover and collect electronically stored physical and/or logical level data from mobile devices.
- Trainee will remove and extract data from removable storage devices in mobile devices.
- Trainee will use forensic analysis tools to filter and sort data based upon file types, dates, special characters, text searches, and password recovery and/or cracking.
- Trainee will use other tools to collect and recover relevant data requested by the stakeholder while maintaining the integrity of the data.
- Trainee will learn how to preview devices at off-site locations (i.e. search warrants) for evidentiary value.

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Required Reading			
Performance Verification of Hardware/Software			
Mobile Device Extractions			
On-Site Forensic Previews			

Module 7 – JTAG/Chip-Off

Required Reading:
JTAG Mobile Acquisition SOP
Chip-Off Mobile Acquisition SOP
Mobile Device Data Extraction SOP

Objectives:

- Trainee will learn proper methods and processes relating to JTAG and chip-off.
- Trainee will learn how to disassemble mobile devices properly depending on which form of analysis (JTAG or Chip-Off) is used.

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Required Reading			
JTAG Acquisition			
Chip-Off Acquisition			

Module 8 – Vehicle Infotainment Analysis

Vehicle Infotainment Analysis is a similar extraction process to mobile devices but utilizes a different software. Because of that, only a software authorization form will be required to perform this type of extraction. This can be added to the casework authorization memo if able to complete in the original training program. Otherwise, a separate software authorization memo will be issued when completed.

Required Reading:
Vehicle Infotainment Analysis SOP
Related Validations/Performance Verifications

Objectives:

- Trainee will attend the Berla iVE training course, if training budget allows. Exceptions can be made in which a trained analyst can provide on the job training.
- Trainee will learn the workflow of how a request for vehicles is made and how the VEB operates.
- Trainee will learn how to navigate the Berla online tools in order to disassemble vehicles and retrieve the infotainment device.
- Trainee will learn how to connect the infotainment device to a workstation in order to extract the data.
- Trainee will learn how to utilize the Berla iVE software to interpret the data.

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Required Reading			
Vehicle Infotainment Analysis			

Module 9 – Administrative and Report Writing

Required Reading:
Reporting Guidelines SOP
Administrative/Quality SOP

Objectives:

- Trainee will learn to document in sufficient detail technical processes and procedures in LIMS and draft a report that meets the HFSC standards for reporting.
- Trainee will learn LIMS and the different applications in LIMS: case creation, chain of custody, item creation, uploading attachments, report writing, technical review, and administrative review.
- Trainee will learn item creation in EMS/Beast.
- Trainee will learn how to complete an effective/appropriate technical and administrative review.
- Trainee will Follow the HFSC Quality Manual requirements for laboratory operations, technical specifications for documentation in the LIMS, and participate in continuous quality improvement activities such as internal audits, offering suggestions for process improvements, corrective actions and/or preventive actions.

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Required Reading			
Administrative and Report Writing			

Module 10 – Legal/Testimony and Ethics

Required Reading:
TFSC Human Factors Reading
TFSC Brady MMA Readings
TFSC Professional Responsibility Readings
HFSC Code of Ethics

Objectives:

- Trainee will follow legal requirements for data preservation.
- Trainee will avoid any action which would result in spoliation of original physical or digital data.
- Trainee will learn how to present findings and evidence in court, affidavits, or during depositions as well as describe the technical processes and procedures for data collection and preservation.
- Trainee will maintain a high degree of personal and professional ethical behavior and protect the confidentiality of technical services and recovered data.
- Trainee will embody ethical standards in technical services, interaction with stakeholders, and maintain a high degree of professional responsibility.

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Required Reading			
Legal/ Testimony and Ethics			

Module 11 – Practical Competency Exam

Upon successful completion of technical training, the section supervisor/lead or manager will administer a competency exam to the trainee. The competency test is a test case and includes a practical application of technical skills and the quality management system requirements (i.e., required level of detail for forensic reporting, and using approved technical methods), and, if deemed necessary, an oral examination of the trainees' ability to define technical processes and terms logically and professionally.

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Computer Competency Test			
Mobile Device Competency Test			
Vehicle Infotainment Software Competency Test			

Module 12 – Written Competency Test(s)

In conjunction with the practical competency exam, a written test will be given to the trainee. The written test will contain questions pertaining to the practical case and the trainee must answer the questions accordingly. A minimum score of 80% is required to pass.

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Computer Written Test			
Mobile Device Written Test			

Module 13 – Supervised Casework

After successful completion of a competency test, the trainee must complete supervised examinations (i.e. processing & analysis) of multiple items to include phones, computers, and removable media. The number of supervised cases completed will based on the trainee’s experience and knowledge. A minimum of 5 supervised cases is required for trainees with previous experience in digital casework. A minimum of 10 supervised cases is required for trainees with no previous experience in digital casework. Due to the limited amount of computer cases the section receives, the minimum number for experienced trainees will be 2 and the minimum number for non-experienced trainees will be 3 supervised cases. These minimum numbers may be adjusted by the trainer due to what casework is available and any adjustments will be noted in the comments section. The trainee will conduct the work under the trainer and the trainer will sign the reports. The trainee's work must be assessed by the trainer and section supervisor/manager based on quality of work product and complexity of analyzed devices.

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Supervised Casework - Computers			
Supervised Casework – Mobile Device (including JTAG/Chip-Off and Vehicle Infotainment)			

Module 14 – Mock Trial(s)

The trainee will complete a mock trial for each area of analysis he/she will be authorized in. This will be arranged by the Multimedia Section. Multiple areas of analysis can be combined in one mock trial if needed (i.e. trainee can do both computer and mobile device testimony in one mock trial).

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Mock Trial - Computer			
Mock Trial – Mobile Device (can include JTAG/Chip Off or Vehicle Infotainment)			

Module 15 – Technical Reviews

The Multimedia Section performs technical reviews on all casework. Authorization of technical reviews will depend on the trainee's prior experience. Trainees with no prior digital casework experience will have to complete at least 15 independent cases prior to starting supervised technical reviews. Trainees with previous comparable digital casework experience can perform supervised technical reviews after supervised casework is completed. Trainees with no experience will complete a minimum of 15 supervised technical reviews. Trainees with previous experience will complete at least 7 supervised technical reviews.

Requirement Category	Trainer Comments	Date Accomplished	Verified By:
Supervised Technical Reviews - Computers			
Supervised Technical Reviews – Mobile Device			